RFC-0012 Continuous Vulnerability Management Standard

Note: FedRAMP requirements documents use RFC 2119 key words to indicate requirement levels.

RFC Front Matter

Due to the nature of this RFC, FedRAMP will be hosting two public events and public informal discussions in the FedRAMP Community about this RFC. General questions are encouraged in these public discussions to sharpen and focus public comment but the public must submit formal public comments for official consideration during the comment period.

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-07-15
- **Closing Date:** 2025-08-21
- **Short Name:** rfc-0012-vulnerability-management

Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: https://github.com/FedRAMP/community/discussions/59
2. Public Comment Form: https://forms.gle/adWgLmR9a4d7vMBW6
3. Email: pete@fedramp.gov with the subject "**RFC-0012 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will not be made public unless requested.

Summary & Motivation

This proposed Continuous Vulnerability Management Standard indicates an intended direction from FedRAMP and is not expected to be finalized in its exact current form. Once the RFC phase is completed, a modified version informed by public comment will be tested and evaluated with volunteer cloud service providers during a 20x Pilot and Rev5 Beta Tests then routinely refined and improved. FedRAMP now works with the community to understand the impact of its policies and adjust them based on real world experiences.

This RFC builds on stakeholder feedback to FedRAMP's recent RFC-0008 Continuous Reporting Standard and incorporates previous plans to update the Continuous Monitoring Performance Management Guide for 20x.

This standard's intent is to ensure providers promptly detect and respond to critical vulnerabilities by considering the entire context over Common Vulnerability Scoring System (CVSS) risk scores alone, prioritizing realistically exploitable weaknesses, and encouraging automated vulnerability management. It also aims to facilitate the use of existing commercial tools for cloud service providers and reduce custom government-only reporting requirements.

This standard implements changes in FedRAMP policy to meet this intent by:

- Defining new plain-language terms to move away from some commonly used but confusing language
- Including all weaknesses in the definition of a vulnerability
- Encouraging urgent mitigation of vulnerabilities prior to remediation

- Establishing requirements for assessing the context of vulnerabilities to determine impact and urgency
- Directly defining potential adverse impact levels
- Prioritizing the discovery, mitigation, and remediation of vulnerabilities in internet-reachable resources
- Setting expectations for continuous assessment, detection, and response where feasible with specific worst-case timelines for vulnerability management
- Requiring POA&Ms only when providers won't respond within the recommended timelines

Reviewers are advised to read through the entire document for the full context and are reminded that FedRAMP 20x definitions for all standards apply to terms in this document; these terms are *italicized* when referenced.

Effective Date(s) & Overall Applicability

This is a draft standard released for public comment; it does not apply to any FedRAMP authorization and MUST NOT be used in draft form.

- FedRAMP **20x**:
  - This standard will initially apply to all FedRAMP 20x authorizations when formalized.
- FedRAMP **Rev5**:
  - See Balancing FedRAMP Rev5 against improvements to FedRAMP 20x for general information how improved FedRAMP standards will be applied carefully and deliberately to Rev5 authorizations.

Background & Authority

OMB Circular A-130: Managing Information as a Strategic Resource defines continuous monitoring as *"maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions."*

The FedRAMP Authorization Act (44 USC § 3609 (a) (7)) directs the Administrator of the General Services Administration to *"coordinate with the FedRAMP Board, the Director of the Cybersecurity and Infrastructure Security Agency, and other entities identified by the Administrator, with the concurrence of the Director and the Secretary, to establish and regularly update a framework for continuous monitoring..."*

Purpose

The FedRAMP Continuous Vulnerability Management Standard ensures FedRAMP Authorized cloud service offerings use automated systems to effectively and continuously identify, analyze, prioritize, mitigate, and remediate vulnerabilities and related exposures to threats; and that information related to these activities are effectively and continuously reported to federal agencies for the purposes of ongoing authorization.

Expected Outcomes

- Cloud service providers following commercial security best practices will be able to meet and validate FedRAMP security requirements with simple changes and automated capabilities
- Third-party independent assessors will have a simpler framework to assess security and implementation decisions that includes consideration of engineering decisions in context
- Federal agencies will be able to easily, quickly, and effectively review and consume security information about the service to make informed risk-based authorizations based on their use case

---

Definitions

FRD-CVM-01

Vulnerability: Has the meaning given in NIST FIPS 200, which is “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”

Note: See also the meaning given to “security vulnerability” in 6 USC § 650 (25), which is “any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of [...] management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.” This includes software vulnerabilities, misconfigurations, exposures, weak credentials, insecure services, and other weaknesses.

Reference: https://csrc.nist.gov/pubs/fips/200/final
Reference: https://www.govinfo.gov/app/details/USCODE-2024-title6/USCODE-2024-title6-chap1-subchapXVIII-sec650

FRD-CVM-02

Credibly exploitable vulnerability: A vulnerability where a *likely* threat actor with knowledge of the vulnerability would *likely* be able to gain unauthorized access, cause harm, disrupt operations, or otherwise have an undesired adverse impact; vulnerabilities must be reachable and not fully mitigated to be credibly exploitable.

FRD-CVM-03

Remediate: Permanently remove a vulnerability; *remediated* vulnerabilities are not exploitable and no longer appear in scans or other analyses.

Note: See also the meaning given to “remediation” in NIST SP 800-216, which is “the neutralization or elimination of a vulnerability or the likelihood of its exploitation.”

Reference: https://csrc.nist.gov/pubs/sp/800/216/final

FRD-CVM-04

Mitigate: Temporarily reduce the risk that a vulnerability will be exploited or the *potential adverse impact* if it is exploited; *mitigated* vulnerabilities still appear in assessments until they are remediated.

Note: See also the meaning given to "mitigation" in NIST SP 800-216, which is "the temporary reduction or lessening of the adverse impact of a vulnerability or the likelihood of its exploitation."

Reference: https://csrc.nist.gov/pubs/sp/800/216/final

FRD-CVM-05

Fully Mitigate: *Mitigate* a vulnerability to the point where there is no reasonable probability of exploitation by any reasonable threat source, or the *potential adverse impact* of exploitation is *Very Low*; *fully mitigated* vulnerabilities still appear in assessments until they are remediated.

FRD-CVM-06

False Positive: Has the meaning given in NIST SP 800-115, which is "an alert that incorrectly indicates that a vulnerability is present."

Reference: https://csrc.nist.gov/pubs/sp/800/115/final

FRD-CVM-07

Internet-reachable: *Information resources* that are reachable over the public internet such that anyone with an internet connection can interact with or deliver payloads to the *information resource*.

Note: This includes *information resources* that have no direct route to the internet but receive or process information or other payloads triggered by internet activity such as some logging services, some application services that process data submitted from internet-facing services, etc.

FRD-CVM-08

Known Exploited Vulnerability: Has the meaning given in CISA BOD 22-01, which is any vulnerability identified in CISA's Known Exploited Vulnerabilities catalog.

Reference: https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities
Reference: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

FRD-CVM-09

Potential adverse impact (of vulnerability exploitation): The estimated effect of unauthorized access, disruption, harm, or other adverse impact to *federal information* that is likely to be caused by a threat actor exploiting a vulnerability. FedRAMP uses the five qualitative values described in NIST SP 800-30 Appendix H, which are:

1. **Very High:** Exploitation could be expected to have multiple severe or catastrophic adverse effects.

2. **High:** Exploitation could be expected to have a severe or catastrophic adverse effect. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii)

result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

3. **Moderate:** Exploitation could be expected to have a serious adverse effect. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

4. **Low:** Exploitation could be expected to have a limited adverse effect. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

5. **Very Low:** Exploitation could be expected to have a negligible adverse effect.

Note: See also NIST FIPS 199 for additional background on measuring Potential Impact on Organizations and Individuals.

Reference: https://csrc.nist.gov/pubs/sp/800/30/r1/final
Reference: https://csrc.nist.gov/pubs/fips/199/final

FRD-CVM-10

Promptly: As quickly as possible and without unnecessary delay.

Requirements

FRR-CVM

These requirements apply ALWAYS to ALL FedRAMP Authorized cloud services based on the current Effective Date(s) and Overall Applicability of this standard.

FRR-CVM-01

Providers MUST establish and maintain programs that meet the requirements and timeframes in this standard to detect, evaluate, report, mitigate, and remediate vulnerabilities; these requirements supplement controls in FedRAMP Rev5 Baselines and Key Security Indicators in FedRAMP 20x.

Note: FedRAMP recommends that providers reference CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) methodology and CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

Reference: https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc
Reference: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

FRR-CVM-02

Providers MUST create and maintain vulnerability reports showing vulnerability management activity that include at least the following information about all detected vulnerabilities within the FedRAMP Authorized *cloud service offering*:

1. Provider's internal unique identifier for the vulnerability or grouping of similar vulnerabilities
2. Relevant Common Vulnerabilities and Exposures (CVE) ID(s) and/or similar public identifiers
3. Timeline (including at least time frames for detection, *mitigation*, and *remediation*)
4. *Internet-reachable* status of affected resources
5. Exploitability assessment (is it *credibly exploitable?*)
6. *Potential adverse impact* assessment
7. *Mitigation* and/or *remediation* plan (including any customer responsibilities)
8. *Mitigation* and/or *remediation* measures taken (including any customer responsibilities)
9. Changelog or other record of updates
10. Point of contact for additional information

Note: This information SHOULD be limited to a minimum level of detail required (see FRR-CVM-07).

FRR-CVM-03

Providers MUST make vulnerability reports available to all necessary parties in similar human-readable and compatible machine-readable formats, including at least FedRAMP, CISA, and all agency customers.

FRR-CVM-04

Providers MUST adjust the risk and severity of vulnerabilities using CVSS base scores (if applicable) AND the context of the vulnerability, factoring for at least criticality, reachability, exploitability, detectability, prevalence, and *mitigation*, to determine if vulnerabilities are *credibly exploitable* and the *potential adverse impact* of exploitation.

FRR-CVM-05

Providers SHOULD *mitigate* and/or *remediate* vulnerabilities promptly, within the time frames established in FRR-CVM-TM, and MUST create a FedRAMP Plan of Action & Milestones (or future equivalent) to address any vulnerabilities that will not be addressed within those time frames.

FRR-CVM-06

Providers SHOULD use automated systems to identify, *mitigate*, and/or *remediate credibly exploitable vulnerabilities* in *internet-reachable information resources* with minimal or no human intervention.

FRR-CVM-07

Providers SHOULD NOT share specific sensitive information about vulnerabilities that would likely lead to exploitation, but MUST share sufficient information about vulnerabilities for oversight, tracking, analysis, action, and risk assessment with all necessary parties.

FRR-CVM-08

Providers SHOULD maintain records of all *false positive* vulnerabilities and exclude validated *false positive* vulnerabilities from vulnerability reports.

FRR-CVM-09

Providers SHOULD group similar vulnerabilities detected across different resources together for tracking, action, and reporting; these groups MUST use sensible provider-defined shared characteristics such as (but not limited to) common root cause, affected component, or remediation strategy.

FRR-CVM-TM

These requirements identify specific time frame-based goals related to continuous vulnerability management.

FRR-CVM-TM-01

Providers MUST provide up-to-date vulnerability reports to all necessary parties at least monthly and SHOULD provide these continuously.

FRR-CVM-TM-02

Providers MUST make historical vulnerability reports covering at least the preceding 24 months available to all necessary parties.

FRR-CVM-TM-03

Providers SHOULD *remediate Known Exploited Vulnerabilities* according to the due dates in the CISA Known Exploited Vulnerabilities Catalog (even if the vulnerability has been *fully mitigated*).

Reference: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

FRR-CVM-TM-04

Providers SHOULD discover, analyze, and assess all *internet-reachable* resources for vulnerabilities using both authenticated and unauthenticated assessments continuously, otherwise at regular intervals at least every three calendar days.

FRR-CVM-TM-05

Providers SHOULD *fully mitigate* or *remediate credibly exploitable* vulnerabilities in *internet-reachable* resources *promptly*, within three calendar days of detection.

FRR-CVM-TM-06

Providers SHOULD discover, analyze, and assess all resources that are NOT *internet-reachable* for vulnerabilities using both authenticated and unauthenticated assessments continuously, otherwise at regular intervals at least once every seven calendar days for unauthenticated assessments and at least once every month for authenticated assessments.

FRR-CVM-TM-07

Providers SHOULD *mitigate* or *remediate credibly exploitable* vulnerabilities in resources that are NOT *internet-reachable promptly*, within seven calendar days of detection, until or unless the *potential adverse impact* is *Low* or *Very Low.*

FRR-CVM-TM-08

Providers SHOULD *mitigate* or *remediate credibly exploitable* impact vulnerabilities in resources that are NOT *internet-reachable promptly*, within 21 calendar days of detection until or unless the *potential adverse impact* is *Very Low.*

FRR-CVM-TM-09

Providers MUST *fully mitigate* or *remediate* all remaining detected vulnerabilities on a regular basis promptly, at least every six months.

Quick Reference - Vulnerability Response Time Frames:

Applies to	Reachability	Impact	Action	Max Time

Credibly exploitable vulnerabilities	Internet-reachable	Very High, High, Moderate, Low	Fully mitigate or remediate	3 Days
Credibly exploitable vulnerabilities	Not internet-reachable	Very High, High, Moderate	Mitigate to Low or remediate	7 Days
Credibly exploitable vulnerabilities	Not internet-reachable	Low	Fully mitigate or remediate	21 Days
All detected vulnerabilities	Both	Very Low	Fully mitigate or remediate	6 Months

Quick Reference - Discovery and Analysis Time Frames:

Assessment Type	Target Resources	Assess At Least
Authenticated	Internet-reachable	Every 3 days
Unauthenticated	Internet-reachable	Every 3 days
Unauthenticated	Not internet-reachable	Every 7 days
Authenticated	Not internet-reachable	Every 1 month

FRR-CVM-AY

These requirements provide guidance on the application of this standard.

FRR-CVM-AY-01

Providers MAY share vulnerability reports publicly or with other parties when doing so will not have a *likely* impact on the confidentiality, integrity, or availability of *federal information*.

FRR-CVM-AY-02

Providers MAY provide additional security relevant metrics in their reporting as they deem appropriate.

FRR-CVM-AY-03

All parties SHOULD follow FedRAMP's best practices and technical assistance on continuous vulnerability management and vulnerability reporting where applicable.

FRR-CVM-EX

These exceptions MAY override FedRAMP requirements for this standard.

FRR-CVM-EX-01

Providers MAY be required to share additional vulnerability information, alternative reports, or to report at an alternative frequency as a condition of a FedRAMP Corrective Action Plan or other agreements with federal agencies.

FRR-CVM-EX-02

Providers MAY be required to provide additional information or details about vulnerabilities, including sensitive information that would likely lead to exploitation, as part of review, response or investigation by necessary parties; providers MUST NOT use this standard to reject requests for additional information from necessary parties which also includes law enforcement, Congress, and Inspectors General.